IN THE SPECIFICATION

Please amend the specification as follows:


Please amend the paragraph beginning at page 7, line 15 as follows:

In this illustration, there are three fundamental entities. A client computer 100 encrypts

data and stores the encrypted data at a server computer 102 in an encrypted client database 104

managed by an application service provider 106. The encrypted client database 104 is augmented

with additional information (which we call the index) that allows certain amount of query

processing to occur at the server computer 102 without jeopardizing data privacy. The client

computer 100 also maintains metadata 108 which is used by a query translator 110 for translating

the user query 112 into different portions, i.e., a query over encrypted data 114, for execution on

the server computer 102, and a query over decrypted data 116, for execution on the client

computer 100. The server computer 102 generates an encrypted intermediate results set 118a,

which is transferred to the client computer 100 and stored as temporary results 120. The client

computer 100 includes a query executor 122 that decrypts the temporary results 120 and

performs the query over decrypted data 116, which may include a filtering or sorting operation,

to generate an updated intermediate results set 118b, which is then re-encrypted and transferred

back to the server computer 102. The server computer 102 completes its query processing on the

re-encrypted intermediate results set 118b, in order to generate a new intermediate results set

118c, which is provided to the client computer 100 and stored as temporary results 120. Finally,

the query executor 122 in the client computer 100 decrypts the temporary results 120 and

performs the query over decrypted data 116 in order to generate actual final results 124, i.e., an

answer to the query, for display 126 to the user.

Please amend the paragraph beginning at page 13, line 3 as follows:

Therefore, the partitioning and query processing strategy used in this application generalizes the approach proposed in along two important directions. First, $Q^S$ executes over the encrypted representation directly generating a (possibly) possible super-set of results. Second, the results of $Q^S$ are decrypted and further processed by the client computer 100 using $Q^C$ to generate the answer to $Q$. We refer to the above partitioning of $Q$ into $Q^S$ and $Q^C$ as operator level partitioning.